State of West Virginia
INFORMATION SECURITY POLICY

GUIDELINES

Issued By:
Governor's Office of Technology
August 1, 2002

INTRODUCTION

1.0.....INTRODUCTION

The Chief Technology Officer (CTO), within the Governor's Office of Technology, is required by State law (1997, c.5) to: "[d]evelop a mechanism for identifying those instances where information should be linked and information shared, while providing for appropriate limitations on access and the security of information." In accordance with this act, State agencies are hereby required to provide for the security and confidentiality of State information and information resources. Each agency shall adhere to the mandates of this Policy.

The State Information Security Policy is a charter document. The Policy guides agencies toward the development of their individual information security programs. Each agency shall complete an information security program consistent with this Policy, and shall submit complete documentation of the program to the Governor's Office of Technology by December 31, 2002. The Policy will be revised as necessary.

Requests for waivers, deviations, or exceptions to this Policy shall be based on general Statute (or equivalent authority) or the results of a risk analysis, and will be subject to approval by the Governor's Office of Technology. The GOT AGREES TO REVIEW AND RESPOND TO ANY AGENCY WITHIN 45 DAYS OF RECEIPT OF A PLAN OR REQUEST, AFTER WHICH THE PROPOSAL IS APPROVED BY DEFAULT. In either event, the GOT will be responsible for responding, in writing, to each agency upon receipt of their security plan or requests as listed above. Further, The GOT will respond to an agency once the plan is accepted or denied.

1.1.....What Is Information Security?

The purpose of information security is to ensure the integrity and availability of information while preventing unauthorized access to it.

Information takes many forms. It can be stored on various media, transmitted across networks, printed out or written down on paper, and spoken in conversations. Appropriate protection should be applied to network infrastructures, databases, disks/diskettes, tapes, optical media, paper, films, slides, models, conversations, and any other methods used to convey knowledge and ideas: All hardware, software and data transmission mechanisms.

There are three basic components of information security:

- *Integrity*: the information is complete and uncorrupted
- *Availability*: the information is accessible to those who need it
- *Confidentiality*: the information is secure from unauthorized access

1.2.....Why Is Action Needed?

State information is under threat. As information grows in volume, complexity, and criticality, and as access to information is broadened, it is increasingly vulnerable. More people can access more data than

ever before, which exposes the data to corruption, destruction, theft, malice, error, and failure.

Information is a valuable State asset. It must be protected as stringently as the State's other assets, both tangible and intangible.

1.3.....Purpose of the State Information Security Policy

a. Establish general standards and policies for information security
b. Initiate the development of information security programs in State agencies
c. Establish management and staff accountability for the protection of agency information resources

1.4.....Scope

This Policy defines common security requirements for all State agencies. The Policy applies to all agency information, to systems that store, access, or process the information, and to agency personnel.

The Policy also applies to information resources owned by others, such as political subdivisions of the State, agencies of the federal government, or entities in the private sector, in those cases where the State has a contractual or fiduciary duty to protect said resources while the resources are in State custody. In the event of a conflict, the more restrictive measures apply.

DEFINITIONS

2.0.....DEFINITIONS

Access means to approach or use an information resource.

Access control is the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Accountability tracking is the process that ensures that the actions of an entity can be traced uniquely to that entity.

Agency means a department, bureau, commission, board, office, council, or other entity in the executive branch of government, which was created by the constitution or statutes of this State.

Application is a computer program used to meet a specific set of information requirements.

Application Owner / Data Owner is the person or persons who is (are) ultimately responsible for an application and its data's viability. This person should have a very active role in the risk analysis process, and the planning for mitigation of risk and vulnerability.

Authentication is the process of verifying the identity of a user.

Authorization is the positive determination by the owner of an information resource that a specific individual may access that information resource.

Chief Information Officer is the person responsible for all information resources within the agency.

Chief Technology Officer is the person responsible for the State's information resources.

CIRT Cyber Incident Response Team

Confidential information is information that is restricted under the provisions of State or federal laws, or is otherwise deemed confidential by the agency.

Data are representations of facts, concepts, or instructions, which can be communicated, interpreted, or processed.

Database is an organized store of data for computer processing.

Encryption is the process of encoding electronic data that makes it unintelligible to anyone except the intended recipient.

Exposure. See *Risk*.

Firewalls are specialized computers and programs, residing in a virtual area between an organization's network and outside networks, which are designed to check the origin and type of incoming data in order to control access, and block suspicious behavior or high-risk activity.

Guardian of an information resource is the agent charged by the resource owner with direct responsibility for the resource.

Host is a mainframe, mid-range, or server computer that mediates access to databases and/or provides other services to a computer network.

Information is the meaning that a human being assigns to data by means of the conventions applied to those data.

Information resources includes both information and the procedures, equipment, facilities, and software that collect, record, process, store, retrieve, display, and transmit the information.

Information security refers to those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

Information Security Officer (ISO) is the person designated by the agency head to administer the agency's information security program. The ISO is the agency's internal and external point of contact for all information security matters.

ISL Information Security Liaison: A person who acts as a local office "arm" of the Information Security Officer.

Intrusion Detection is the task or process of monitoring traffic on a network, placing sensors in carefully selected locations, to detect abnormalities or variants to normal traffic that might indicate the presence of activity that is unwanted, such as an attack or other form of unwelcome intrusion. Generally, intrusion detection is not effective unless it is monitored 24x7x365. Intrusion Detection standards need to be established to ensure consistency across agencies.

Password is a string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

PC is the abbreviation for Personal Computer: a computer designed for individual use rather than for use as a shared resource such as a mainframe, mid-range, or server computer.

Penetration Testing is the process of launching a simulated incursion into a network to see if access to servers, network switches, routers, or other communications equipment can be discovered, entered, changed, disrupted, or otherwise compromised. The goal is to provide insights that will lead to reduced vulnerability to penetration, theft, denial of service attacks, or other damage to the integrity of information systems' infrastructure, applications, or data.

Provider is an internal or external supplier of information resources.

Risk (also known as *Exposure*) is the likelihood or probability that a loss of information resources or a breach of security will occur. Also, the "value" that can/may be lost or compromised, as in, that which is at-risk. Quantitative/ qualitative measure that assists with prioritizing risk mitigation

Risk analysis is the evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

Safeguards are the protective measures and controls prescribed to meet the security requirements specified for a system. Safeguards may include, but are not necessarily limited to: hardware/software security procedures, operating procedures, accountability procedures, access and distribution controls, personnel security, and physical security.

Security controls are the hardware, programs, procedures, policies, and physical safeguards that are put in place to assure the integrity of information and to protect the means of processing information.

Security incident (also known as *security breach*) is an event that results in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.

Sensitive information is agency information that requires special precautions to protect it from unauthorized access, disclosure, modification, or deletion.

Spoofing is the act of using a network node to launch an attack from a remote location, therefore preserving anonymity of the origination of the attack.

Terminal/Workstation is an instrument through which data or information can enter or leave a computer.

Third party is a non-State entity that performs IT (information technology) services for, or otherwise maintains a network-to-network connection with, a State agency.

Threat includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.

Unit is a branch of an agency. An example would be a division or office of a department or bureau.

User is a person authorized to access an information resource.

Virus is an unauthorized self-replicating program that can interfere with, corrupt, or destroy programs and data. Viruses can infect (transfer to) systems locally via magnetic and optical media, or remotely through computer networks.

Vulnerability is a weakness in the defense or protection of a system component or access point. Examples include such conditions as default configurations, out-of-date patches, poorly chosen passwords, poor physical security, etc.

MANAGEMENT and STAFF RESPONSIBILITIES

3.0.....MANAGEMENT AND STAFF RESPONSIBILITIES

Information security requires the active support and ongoing participation of individuals from various disciplines and all management levels. This section defines the security roles and responsibilities of both management and staff.

3.1.....Agency Heads

The implementation of a security program is ultimately the responsibility of the head of the agency. The agency shall assign the function of agency Information Security Officer (ISO) and shall prescribe the duties and responsibilities of the function.

The ISO function may or may not warrant a dedicated, full-time position, depending on the scope and needs of the agency. Written notification of ISO appointments and changes shall be sent promptly to the Governor's Office of Technology.

The agency head shall ensure that adequate resources are applied to the information security program, and shall ensure that the program is successful.

3.2.....Information Security Officer

The Information Security Officer shall have direct responsibility for establishing and administering the agency's information security program. The ISO function should be located at the policy development and enforcement level of the agency organizational hierarchy.

The ISO shall have the following related responsibilities:

- establish agency-wide information policies and standards
- direct and manage the agency security program
- develop and sustain the agency information risk analysis process
- monitor, investigate, and resolve security violations and generally not policy violations
- monitor an inventory (normally maintained by the operations arm of the agency) of the agency's information resources that have inherent security relevance
- promote awareness of agency responsibilities for information security
- consult with agencies and information technology services groups on information security issues and techniques
- ensure that adequate backup procedures are established, tested, followed, and logged / documented.
- ensure that security is part of the information planning process
- monitor the implementation of security measures for new systems or services
- keep management aware of technical, legal, and regulatory changes affecting information security and computer crime
- evaluate and recommend system security technology tools

- ensure that access authorization procedures are implemented
- provide / plan (including test) for adequate / appropriate incident response(s) of various types (natural disaster, manmade disaster, etc.)

3.3.....Information Security Liaison

Larger agencies should designate a person, or persons, within each unit (e.g. division, section, or branch office of a department or bureau) to serve as the unit's Information Security Liaison (ISL).

The Information Security Liaison should have the following responsibilities:

- assisting the Information Security Officer in conveying information related to the protection of information resources, including general elevation of security awareness in the ISL'S work locale.
- assisting in the detection of actual and potential security exposures, and in responding to security incidents, including, but not limited to: performing periodic and random day audits for logged-on , unattended workstations, and night audits for passwords available to auditor, confidential information left unlocked, and other potential exposures)
- ensuring that the Information Security Officer is immediately notified if an employee transfers to a new job, is dismissed or resigns, or if a new employee is granted access privileges
- monitoring an inventory of the unit's information resources, relevant to information security.
- performing periodic reviews of user access to ensure that all accesses are current and appropriate
- maintain a cognizance with respect to internal threat conditions.
- respond in priority fashion to any urgent requests issued by the ISO, ISO equivalent, or the ISO designate.

AGENCY
INFORMATION SECURITY POLICY

4.0.....AGENCY INFORMATION SECURITY PROGRAM

Each agency shall develop, implement, and maintain an information security program. The program shall be documented and the documentation shall be subject to review and approval by the Governor's Office of Technology. The first such program shall be submitted to the Governor's Office of Technology, for review and approval, on or before July 3, 2000. Programs shall be submitted biennially thereafter. Especially sensitive information should be omitted from the submitted material, and referenced in general terms instead. Program documentation should be treated, and prominently marked, as confidential material.

Some agencies, such as the Department of Military Affairs and Public Safety, and the Department of Tax and Revenue, have extraordinary security considerations and responsibilities. Agencies may implement additional security measures, beyond those identified in this Policy, as part of their information security programs.

The agency information security program shall uphold the policies, standards, and guidelines of this Policy and of the State of West Virginia Technology Master Plan.

The agency information security program shall address, at a minimum, the core components described in sections 4.1- 4.4, below. The components are more fully discussed elsewhere in this Policy, along with other standards and guidelines.

In order to have uniform standards and classification of information / data exchanged between agencies, it is thought that baseline statewide information / data classification and handling standards / procedures need to be developed.

As well, it is thought that information security policy should be created that becomes the default policy for all agencies that are not able to develop their own policies.

4.1.....Administration

Security administration is the management of the agency security program's operational procedures, security education program, compliance with security controls, and security risk assessments. Security administration shall include, at a minimum, the following elements:

- an Information Security Officer assigned to implement and oversee the security program
- a documented agency information security program
- documented procedures for the operation of the security program

- a security awareness program
- a documented risk analysis program
- provisions for security program compliance and incident investigation

4.2.....Information Security

To ensure that the agency effectively manages the risks to the information resources in its custody, access to those resources must be strictly controlled. Access controls shall be consistent with state, federal, and local laws and statutes, and shall be implemented in accordance with this Policy.

In establishing information security procedures, the agency shall:

- establish methods to grant, deny, or revoke, privileges to access data, information, service, and resources
- establish processes to uniquely identify each user
- establish methods to satisfactorily authenticate the identification of the user
- establish processes for accountability and tracking

4.3.....Personnel Practices

Each agency shall implement the following personnel practices:

- establish hiring practices to review user background for possible security risks based upon a thorough review of agency classifications and an assessment of which positions require trustworthiness and confirmation or reconfirmation of that trustworthiness.
- document user duties and responsibilities
- develop, require users to sign, and retain, appropriate agreements. pertaining to confidentiality, security and acceptable use
- consider information security implications in employment termination procedures
- certain positions may require additional background checks and signed agreements pertaining to confidentiality, security and acceptable use.

4.4.....Physical and Environmental Security

The agency shall:

- establish appropriate controls on access to facilities and resources
- ensure the physical security of media containing ALL data maintained by the agency.
- provide, as required, secure facilities for the preparation, collection, and distribution of all data maintained by the agency
- determine security vulnerabilities
- establish controls to detect, and respond to, threats to facilities and physical resources
- consider preventative, detective, and environmental factors in the selection, design, or renovation of facilities that house information resources

INFORMATION SECURITY

5.0.....INFORMATION SECURITY

Agencies shall implement procedures to protect information resources from accidental, inadvertent, unauthorized, or malicious disclosure, modification, or destruction. Agencies shall also implement procedures to shield information resources from access-denial and access-manipulation (e.g. a denial-of-service attack).

5.1.....Authorization

Agencies shall consider all of the following standards of authentication practices and implement based on their specific situations and environments. For example, public systems used in the library may not require certain levels of authorization for use by the general public.

- Information resources shall be protected by use of access control systems. Access control systems should include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).
- Rules for access to resources (including internal and external telecommunications and networks) shall be established by the information/application owner or manager who is responsible for the resources.
- When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.
- Information security and audit controls shall be incorporated into new systems.
- Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.
- General access to systems and data shall be subject to approval by the user's manager.
- When employees are transferred or their employment is terminated, their userids and authorizations shall be deleted immediately. The manager of the particular employee shall promptly inform the unit's ISL, or the agency's ISO, of the termination or transfer.
- Users should be classified as either:

  - privileged users, such as the system administrator and other special userids (which should be documented and authorized by management)

  - users with data entry/update capabilities

  - users with inquiry capabilities only

- Standards for data testing:

  - Testing shall be performed in a test environment that is kept separate from the production environment.

  - Testing shall be performed only on test data in a test environment. Production data may be copied into the testing environment, but appropriate controls shall be placed on the disclosure of production data that has been copied.

  - Changes to production data shall be subject to approval by the responsible owner.

  - Production programs shall be kept in controlled files.

  - Application development programmers shall not update production libraries without authorization from the owners of those libraries.

  - Procedures shall be developed and implemented to ensure that the development or change of production programs is done in an organized and controlled manner.

  - Documentation shall be completed or updated before a program change is moved into the production environment.

- Programming Standards:

  - Agencies that engage in application development should adhere to programming standards which provide for the appropriate application level security elements.

5.2.....Authentication

Agencies shall establish and maintain standards of authentication. The following means shall be used to corroborate, prove, or confirm the identity of the user: If an agency has legitimate reason to not follow any of these standards, they shall document same and submit with their agency plan.

Passwords

- Passwords shall be changed periodically, with period not to exceed 45 days.
- Expiring passwords shall be used for critical resources.
- Passwords should be of certain minimum (no fewer than 8) and maximum character lengths, in a combination of alphabetic and numeric characters.
- Passwords should not be trivial or predictable. (e.g. no dictionary words found in any language, or spelled backwards in any language. Passwords should include a numeric or special character placed in other than the third character position. Passwords should be case sensitive, etc.
- Compromised passwords shall be changed immediately.

- Passwords shall not be shared.
- Passwords should be selected by the user. When initial passwords are assigned or passwords are reset, the user should be instructed, or automatically prompted, to manually change that assigned password.
- Passwords shall be kept confidential.
- Access to the password file shall be limited and strictly controlled.
- Passwords shall be masked or suppressed on all online screens, messages, printed output, reports, and logs.
- Passwords stored on a computer shall be encrypted.
- Passwords sent over a computer network should be encrypted.
- Personal digital assistant (pda) devices that are synchronized with personal computers, or that contain critical / sensitive or confidential data must be password protected.

Tokens

Authentication standards can vary according to the type of token used. Examples are memory tokens (magnetic striped card) and smart tokens (cards with built-in integrated circuits). If the security need warrants such authentication, token attributes should be never shared.

Biometrics

Authentication can be established by physiological attributes (fingerprints, retinal patterns, etc.) or behavioral attributes (voice patterns, hand-written signatures). If the security need warrants such authentication, machines and supporting software shall be procured and applied. In such cases, all legitimate users shall be enrolled in a database, based on the physical attribute the machine measures.

5.3.....User Identification

Individual users shall have unique logon IDs (userids) and passwords. An access control system shall identify the user and prevent unauthorized users from entering/using information resources.

Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall not allow others to use their userids.
- Users shall be responsible for the use/misuse of their individual userids.
- A single userid shall not be permitted to sign on to a system or application from more than one physical workstation at a time, except for authorized computer support personnel for the purposes of testing/troubleshooting.
- Inactive userids shall be revoked after a 90 day maximum period of disuse, except under special circumstances.
- The userid shall be locked/revoked after a maximum of three (3) unsuccessful logon attempts. Password reset should require administrative intervention. The agency may impose tighter control if desired.
- Terminals shall not be left unattended. Unattended terminals should be automatically deactivated (timed-out) after a period of disuse. The system administrator or manager should determine the appropriate deactivation time for the application/session.
- Audit trails should be maintained to account for all accesses to confidential or sensitive information and software, and for all changes to automated security or access rules.

- Logs of access and attempted access should be maintained.
- Violation reports shall be generated and responsible personnel shall monitor the reports.
- The actions of a user should be traceable to that user.
- When an employee leaves an organization, their accounts / access privileges should be disabled immediately, and revoked after a specified interval of time.

5.4.....Computer Viruses

Agencies shall develop and implement procedures for system protection by acquiring, installing, and using virus protection software on all personal computers and servers. These procedures shall also address the downloading of information from communication links such as the Internet and private access services. Techniques such as automatic pushing of anti-virus software updates, real-time scanning, automatic scheduled scanning, e-mail scanning tools, centralized scan management, and automatic daily updates, should all be utilized to ensure the success of anti-virus measures.

5.5.....Data and Software Backup

Data and supporting software essential for the continuation of agency functions shall be backed up. The security controls over the backup resources shall be as stringent as the security controls applied to the primary resources.

The agency shall ensure that at least two employees are familiar with the content and location of the data files and supporting software, and with the proper sequence of operations for setting up the software and restoring the data in case of an emergency. Staffing plans and procedural documentation should be provided to the ISO or ISO equivalent / designate.

Test restore procedures should be performed annually at a minimum for all systems and data sets. Test documentation should be provided within 2 weeks of tests to ISO or ISO equivalent / designate.

RISK ANALYSIS

6.0.....RISK ANALYSIS

Absolute security is unachievable and not realistic, nevertheless, potential losses must be weighed against risk factors and the value of the information and its accessibility to the mission of the agency. In doing this, an agency must develop a risk mitigation plan through the use of risk analysis.

A risk analysis, by qualified evaluators, and involving the application / data owners, is imperative to properly assess overall risk and determine a course of action to alleviate or minimize those risks identified.

Overall risk considers 1) the likelihood that a threat will breach a vulnerability, as well as 2) the value of the asset, i.e., a quantification of the loss, possibly in dollars, of the loss resulting from that breach in terms of lost worker productivity (wages), cost of recovery from the problem, and even non-dollar cost such as political exposure and other ramifications.

Potential losses must be weighed, and the expenditure on security controls must be balanced against the value of the information resource, and the consequences that could ensue from its loss or inaccessibility.

The Information Security Officer shall conduct periodic risk analyses to address the changing organizational priorities and threats to information. The analyses shall be conducted with sufficient regularity to ensure realistic responses to current risks. (e.g., agencies with sensitive data should do this quarterly or semi-annually, and agencies with minimal sensitive data may find annual reviews are sufficient.)

Results of the risk analyses shall be documented, and that documentation shall be included as part of the agency's documented information security program. The documentation should be considered sensitive and potentially confidential and be treated accordingly.

The risk analysis may vary from an informal, but documented, review of a microcomputer or terminal installation to a formal, fully quantified risk analysis for a large computing environment.

At a minimum, risk analysis involves consideration of the following factors:

- A) the nature of the information and systems
- B) the business purpose for which the information is used
- C) the environment in which the system is used and operated
- D) the protection provided by the controls in place
- E) the organizational consequences that would likely result from a significant breach of security
- F) the realistic likelihood of such a breach occurring in the light of prevailing threats and controls
- G) the determination of which information resources are to be protected, and to what extent

Risk Analysis Process

1) Identify all systems in the Agency or Department that merit analysis.
2) For each system identified in Step 1, document A, B, C and D above
3) For each system identified in Step 1, document the consequences of that would result from a loss of system functionality, availability, integrity (lost worker wages, political fallout, etc).
4) For each system identified in Step 1, document a best-estimate of the likelihood of an out-of-service condition resulting from natural disaster,
human error, malicious attack or other system or infrastructure failure.
5) Complete a funded plan to mitigate vulnerabilities for those systems identified as critical and where mitigation is justified by risk determined.
6) For each system analyzed, determine an appropriate frequency for a review of the risk analysis, and set the date for the next review.
7) Perform reviews according to the schedule developed in Step #6.
8) Provide complete documentation as developed above to ISO and/or application / data owner, or agency head, as agreed.

ACCOUNTABILITY FOR INFORMATION RESOURCES

7.0.....ACCOUNTABILITY FOR INFORMATION RESOURCES

All major information assets shall be accounted for and shall have an assigned guardian.

7.1.....Inventory of Resources

The Information Security Officer shall monitor an inventory of the information resources of the agency. Unit Information Security Liaisons, if designated, shall assist in this effort. Each information resource, and its guardian /owner, shall be documented. The following are examples of information resources:

Information - databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements

Software - application software, system software, development tools and utilities

Hardware - computer and communications equipment, power supplies, air conditioning units

Services - computing, communications, and facilities services required for operation

7.2.....Resource Guardians

Critical information resources shall be assigned a guardian. Guardians shall protect their assigned resources. The guardian or the guardian's supervisor shall report any change in resource inventory to the unit's Information Security Liaison or the agency's Information Security Officer.

7.3.....Disposal of Information Resources

Agencies shall adhere to the following guidelines when disposing of information resources:

Hardware - Agencies shall observe the rules and regulations of the Surplus Property Unit, Purchasing Division, and Department of Administration. Items of equipment containing storage media should be checked to ensure that sensitive data are adequately overwritten prior to disposal.

Software - Authorized personnel shall dispose of software and remove any licensed copies of the software from the corresponding hardware. Disposal of software shall conform to the software publisher's, or manufacturer's, license agreements or copyright agreements, if available. Operating systems “belong” with the personal computer and application software may generally be passed to another user with a personal computer, so long as that software is not retained for use by the person relinquishing the equipment.

SECURITY OF THIRD PARTY ACCESS

8.0.....SECURITY OF THIRD PARTY ACCESS

The security of State systems can be jeopardized from third party locations if State security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of State systems. The Information Security Officer, information resource management, and State legal counsel should be involved in the process.

Third party access to State systems should not be granted until all these concerns have been addressed and a contract defining the terms of the connection has been signed.

8.1.....Emphasis on Security in Third Party Contracts

Third party access to State systems should be based on a formal contract containing all terms and conditions necessary to ensure compliance with State and agency information security policies and standards. The following items should be considered for inclusion in such contracts:

- applicable sections of the State Information Security Policy
- policies and standards established in the agency's information security program
- the liabilities of the parties to the agreement
- the right to audit contractual responsibilities
- arrangements for reporting and investigating security incidents
- a description of each service to be made available
- a requirement to maintain a list of individuals authorized to use the service
- permission to screen authorized users
- the dates and times when the service is to be available
- procedures regarding protection of information resources
- the right to monitor and revoke user activity
- restrictions on copying and disclosing information
- responsibilities regarding hardware and software installation and maintenance
- measures to ensure the return or destruction of programs and information at the end of the contract
- any required physical protection measures
- an authorization process for user access
- mechanisms to ensure that security measures are followed
- user training in security procedures
- measures to prevent infection by viruses, Trojan horses, and similar hazards to information resource integrity

---

RESPONDING TO INCIDENTS

9.0.....RESPONDING TO INCIDENTS

9.1.....Reporting Security Incidents

Reports of security incidents shall be escalated as quickly as possible. A formal incident response procedure, defining the action to be taken upon receipt of an incident report, shall be developed by the Information Security Officer. Users and/or guardians shall be instructed to inform appropriate parties in the event of a security incident. This should initially be done via a Help Desk if the agency has such a facility.

Security breaches shall be promptly investigated. If criminal action is suspected, the agency shall contact the appropriate law enforcement and investigative authorities immediately.

9.2.....Reporting Security Weaknesses

Users should note and report any observed or suspected information security exposure. The Information Security Officer should promulgate this policy as part of the agency's information security program. Users should be given clear instructions on how to report such weaknesses. Users shall not attempt to prove a suspected weakness, as this might be construed as a misuse of the system.

9.3.....Reporting Software Malfunctions

Users should inform the Help Desk or a designated individual when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk.

If the user, or the user's manager or supervisor, suspects a computer virus infection, the agency's computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer. Do not carry out any commands, including commands to Save data. Do not close any of the computer's windows or programs. Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate Help Desk or the agency's Information Security Officer or the unit's Information Security Liaison as soon as possible.
- Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use, which preceded the malfunction.
- Do not attempt to remove a suspected virus! Use the Help Desk to contact staff trained in virus control.

The Information Security Officer or Information Security Liaison should monitor the resolution of the malfunction or incident.

RESPONSIBILITIES OF PERSONNEL

10.0.....RESPONSIBILITIES OF PERSONNEL

10.1…..User

The user of an information system or asset is responsible for the day-to-day, hands-on security of that system or asset. The user shall report known or presumed security vulnerabilities, risks, threats and incidents to the unit's Information Security Liaison or the agency's Information Security Officer.

The agency owns all information technology assets, including hardware, software and data used by agency staff. These assets include e-mail, hard drive space, network bandwidth, activity logs and all backup copies of e-mail, activity logs and other data.

Privacy for employees does pose an issue in specific circumstances. For example, state physicians are involved with the transmission and storage of privledged information that not just anyone can be privy to. With this in mind, the practices outlined here must be treated as a guideline and applied accordingly. However, for the most part, much of what state government is involved with is subject to rules governed by the freedom of information act and can be viewed when requested by proper methods outlined by the foia law.

10.2.....Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this Policy. Agencies may expand the list:

- *Crashing an information system*. Deliberately crashing an information system is prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user will be viewed as a possibly deliberate act.
- *Attempting to break into an information resource or to bypass a security feature*. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- *Introducing, or attempting to introduce, computer viruses, Trojan horses, or other malicious code into an information system.*

Exception: Authorized information system support personnel, or others authorized by the agency's CIO or ISO, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

Additional prohibitions:

- *Copyright violation*. This includes the act of pirating software, or the use of pirated software, and the illegal duplication or promulgation of information and other intellectual property that is under copyright.

- *Illegal activities*. Use of State information resources for, or in support of, illegal purposes as defined by federal, State, or local law.
- *Commercial use*. Use of State information resources for personal or commercial profit.
- *Browsing*. The willful, unauthorized access or inspection of confidential or sensitive information.
- *Personal or unauthorized software*. Use of such software is prohibited.
- *Political activities*

10.3.....Use of Organizational Resources

State information resources are designated for authorized purposes. To maintain and manage these resources, the State reserves the right to examine all data stored in, or transmitted by, such resources.

All software programs and documentation purchased for the use of the State are State property and shall be protected as such.

10.4.....Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the State are the property of the State unless excepted by contractual agreement. Agencies should ensure that all workers developing programs or documentation sign a statement acknowledging State ownership before they start such work. Nothing contained herein applies to software purchased by State employees at their own expense.

10.5.....Internet Considerations

Special precautions shall be taken when a State information resource has access to the (public) Internet. The precautions are needed to block access to all State information resources not intended for public access, and to protect confidential State information when it is to be transmitted over the Internet.

Each agency shall develop and promulgate an acceptable usage policy governing the use of the Internet connections to its resources. Such policies shall address security issues, including:

- Prior approval of the agency Chief Information Officer, Information Security Officer, or other individual authorized by the agency shall be obtained before:

  a. an Internet, or other external network connection, is established;

  b. State information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server).

- All software downloaded via the Internet shall be screened with current virus protection software.
- In instances where the content or reliability of downloaded software is in doubt, the software should be tested on a standalone non-production computer.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the agency's Chief Information Officer, Information Security Officer, or

other individual authorized by the agency. The use of encryption software and keys which have not been escrowed as prescribed above is prohibited, and may make the user subject to disciplinary action.

10.6.....Mention of Information Security in Job Descriptions

Information security roles and responsibilities should be included in job descriptions where appropriate.

10.7.....Screening of Job Applicants

Applications for employment - whether of permanent or temporary State employees, or independent contractors - should be screened if the job entails special trust or responsibility, work within sensitive areas, or access to critical or sensitive information. At a minimum, the following checks should be made:

- at least two satisfactory character references
- a check of the applicant's resume for completeness and accuracy
- confirmation of academic and professional qualifications
- an identification check (e.g. passport or birth certificate)

10.8.....Confidentiality Agreement

Users of State information resources shall sign, as a condition for employment, an appropriate confidentiality or non-disclosure agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on State information resource systems may result in disciplinary action consistent with the policies and procedures of federal, State, and local agencies.*

Temporary and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing State information resources.

Confidentiality agreements shall be reviewed when there are changes in contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

EDUCATION and TRAINING

11.0.....EDUCATION AND TRAINING

Security awareness, including the training of information resource custodians, users, providers, and management, is one of the most effective means of reducing vulnerability to error and fraud, and must be continually emphasized and reinforced.

The Information Security Officer of the agency shall develop and implement a continual security education/training program including at least the following elements:

- All users shall receive appropriate training in policies and procedures, including security requirements and other organizational controls, as well as training in the correct use of information resources (e.g. logon procedure, use of software packages, and changing of passwords). New employees shall receive such training before access to information resources is granted. Information resource guardians, users, providers, and their management shall be informed of their respective responsibilities for information resource protection and recovery. These responsibilities shall be clearly defined.
- Information resource guardians, users, providers, and their management shall be informed of the consequences of non-compliance with their security responsibilities. These consequences shall be clearly stated.
- Information resource guardians, users, providers, and their management shall be informed of the provisions of this Security Policy, the provisions of the West Virginia Computer Crime and Abuse Act (1989, c.47), any other relevant federal or State statutes, and security policies and standards that have been established by the agency.
- Employees shall acknowledge and accept, in writing, the agency's defined security policies, procedures, and responsibilities. The Information Security Officer shall ensure that the agency maintains records to this effect.

PHYSICAL and ENVIRONMENTAL SECURITY

12.0.....PHYSICAL AND ENVIRONMENTAL SECURITY

12.1.....Physical Security of Information Resource Facilities

Information resource facilities shall be physically secured by measures appropriate to their critical importance. The following options should be considered:

- The selection and design of the facility should minimize the risk of natural, accidental, or intentional disasters.
- Physical security should be based on defined perimeters and achieved through a series of barriers located strategically throughout the organization.
- Critical facilities should be located away from areas of public access, including direct approach by public vehicles.
- Critical facilities should be unobtrusive, with no obvious signs, outside or inside the building, identifying the presence of computing activities.
- Critical facilities should not be identified in telephone directories (public or internal) or lobby directories.
- Backup equipment and storage media should be located at sufficient distance to avoid damage in case of a disaster at the main site.
- Appropriate safety equipment, such as heat and smoke detectors, fire alarms, and fire extinguishing equipment, should be installed, and checked regularly. Employees should be trained in the use of safety equipment and in evacuation procedures.

12.2.....Protection Outside of Secure Areas

Critical or sensitive data that are handled by terminals/workstations, communication switches, and network components outside of secure areas shall receive the level of protection necessary to ensure their integrity and confidentiality. The required protection may be achieved by physical or logical controls.

12.3.....Equipment

Critical information resource equipment shall be secured, and should be protected from fire, smoke, water, dust, vibration, chemical effects, electrical interference, and electromagnetic radiation.

12.4.....Power Supplies

Equipment should be protected from power failures and other electrical anomalies. An uninterruptible power supply (UPS) shall be used for equipment supporting critical operations. Contingency plans

should address a course of action to pursue after the UPS is exhausted (e.g. systematic shutdown of unattended resources). UPS equipment should be regularly serviced and tested.

12.5.....Cabling

Power and telecommunication cabling carrying data or otherwise supporting information resources should be protected from interception or damage. The following measures should be considered:

- Shielded cabling.
- Power and telecommunications lines into information resource facilities should be underground or should be provided alternative protection.
- Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.
- For exceptionally sensitive or critical systems, consideration should be given to additional measures such as:

  - use of data encryption

  - installation of armored conduit and locked rooms

  - use of alternative routing or transmission media.

12.6.....Equipment Off-Premises

Information resource equipment used outside State premises to support State activities e.g. (employee sign-on to state from home) shall be given the same degree of security protection as that of on-site information resource equipment. The following measures shall be applied:

- When personal computers are used at home or other off-site premises, for purposes of State business, virus controls shall be in place.
- Equipment and media shall not be left unattended in public places. During travel, portable computers shall be carried as hand luggage.
- Portable computers shall be given an appropriate form of access protection (e.g. passwords or encryption) to prevent unauthorized access to their contents.
- Outside connections to state networks should be through a VPN whenever possible.

NETWORK SECURITY

13.0.....NETWORK SECURITY.

A range of security controls is required for computer networks. During transfer, data are particularly vulnerable to both unintentional and deliberate access and/or alteration.

13.1.....General Network Controls

Network resources accessing confidential information shall assume the confidentiality of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk, and shall include at least the following:

- Routers, critical servers, PBXs, and communications controllers shall be protected from unauthorized physical access.
- Access to diagnostic ports shall be securely controlled.
- The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session shall pass through said authorizations.
- No Network-to-Network connections shall be attempted or implemented without the prior approval of management.
- Connections by remote computer systems shall be subject to authentication.
- Access to information shall be based on the need for the information, or the need to maintain and administer the information resource.
- When appropriate, techniques shall be employed to ensure verification (non-corruption of data). Examples are character counts, error detection and correction (protocols).
- Unauthorized attempts (successful or unsuccessful) to access or modify data through a communication network shall be promptly investigated.
- If unauthorized access or modification of data occurs, the agency shall promptly review its existing security measures, and add new measures or modify existing measures.
- If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks.
- When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the agency owning the data shall establish the criteria.

The following additional controls should be considered:

- Line junction points should be located in secure areas, preferably under lock and key.
- Keys should be transmitted separately from the encrypted information, preferably through different channels.
- Passwords should be encrypted during transmission and in storage.
- Users should be provided with direct access only to the services that they have been specifically authorized to use.

13.2.....Dial-Up Access

The following guidelines should be considered:

- Access to agency information resources through modems or other dial-in devices/software should be subject to authorization and authentication by an access control system. Direct inward dialing without passing through the access control system should be prohibited.
- Dial-up numbers should be unlisted.
- Dial-up facilities should be equipped with either an automatic hang-up and call-back feature (with call-back to authorized callers only) or authentication systems that employ tokens.
- Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems should have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

13.3.....Enforced Path

The objective of an enforced path is to prevent any undesirable straying by users outside the route between the user workstation and the service that the user is authorized to access. This usually involves controls at several points in the route. The principle is to limit the routing options at each point in the network, through predefined choices. The following controls should be considered:

- allocating dedicated lines or telephone numbers
- automatically connecting ports to specified application systems or security gateways
- limiting menu and submenu options for individual users
- preventing unlimited network roaming

13.4.....Segregation of Networks

Large networks may need to be separated into separate domains. In such circumstances, network segregation controls should be considered. One such method is to divide large networks into separate logical domains, each protected by a defined security perimeter or firewall, and a network gateway. Access between domains can then be controlled through secure gateways that incorporate appropriate routing and connection-capability controls.

COMPUTER PROGRAM CHANGE MANAGEMENT

14.0.....COMPUTER PROGRAM CHANGE MANAGEMENT

Formal program change management procedures are necessary to ensure that information resource security and controls are not compromised.

- Change requests should originate from, and be documented by, those responsible for the function supported by the data. Change request forms should be reviewed and authorized by end-user management before the forms are submitted to the programmers for change.
- Change requests should be tracked, scheduled, completed, and moved into production by authorized personnel.
- Only authorized personnel should make modifications or overlays to programs in the production or testing areas.
- Testing and development should be separated from the production processing environment to prevent erroneous updating to production data.
- Users should be actively involved in the testing process and should signoff on acceptance of the change before the change is moved to production.
- Data integrity should be adequately addressed in all application integration exercises.

Additional change procedures may include:

- maintaining a record of agreed-upon authorization levels, including:

  - user authority for submission of change requests

  - user authority for acceptance of completed changes

- accepting only those changes submitted by authorized users
- reviewing security controls and integrity procedures to ensure that they will not be compromised by the changes
- identifying all software, hardware, files, and database entities that require revision
- obtaining approval for detailed proposals before work begins
- ensuring that system documentation is updated when changes are completed, and that old documentation is archived or disposed of
- maintaining a version control log of all software updates
- maintaining an audit log of all change requests
